Cisco 2851 Integrated Services Router with AIM-VPN/EPII-Plus

FIPS 140-2 Non Proprietary Security Policy
Level 2 Validation

Version 1.6

September 08, 2008

Table of Contents

1 Introduction

1.1 Purpose

This document is the non-proprietary Cryptographic Module Security Policy for the Cisco 2851 Integrated Services Routers with AIM-VPN/EPII-Plus installed. This security policy describes how the Cisco 2851 Integrated Services Routers (Hardware Version: 2851; Firmware Version: IOS 12.4 (15) T3) meet the security requirements of FIPS 140-2, and how to operate the router with on-board crypto enabled in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the Cisco 2851 Integrated Services router.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at http://csrc.nist.gov/groups/STM/index.html.

1.2 References

This document deals only with operations and capabilities of the 2851 routers with AIM modules in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the routers from the following sources:

The Cisco Systems website contains information on the full line of Cisco Systems routers. Please refer to the following website:

http://www.cisco.com/en/US/products/hw/routers/index.html

For answers to technical or sales related questions please refer to the contacts listed on the Cisco Systems website at www.cisco.com.

The NIST Validated Modules website (http://csrc.nist.gov/groups/STM/cmvp/validation.html) contains contact information for answers to technical or sales-related questions for the module.

1.3 Terminology

In this document, the Cisco 2851 routers are referred to as the router, the module, or the system.

1.4 Document Organization

The Security Policy document is part of the FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

Vendor Evidence document
Finite State Machine
Other supporting documentation as additional references

This document provides an overview of the routers and explains their secure configuration and operation. This introduction section is followed by Section 2, which details the general features

and functionality of the router. Section 3 specifically addresses the required configuration for the FIPS-mode of operation.

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Submission Documentation is Cisco-proprietary and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cisco Systems.

2 Cisco 2851 Routers

Branch office networking requirements are dramatically evolving, driven by web and e-commerce applications to enhance productivity and merging the voice and data infrastructure to reduce costs. The Cisco 2851 routers provide a scalable, secure, manageable remote access server that meets FIPS 140-2 Level 2 requirements. This section describes the general features and functionality provided by the routers. The following subsections describe the physical characteristics of the routers.

2.1 The 2851 Cryptographic Module Physical Characteristics

Figure 1 – The 2851 router case

The 2851 Router is a multiple-chip standalone cryptographic module. The router has a processing speed of 450MHz. Depending on configuration, either the installed AIM-VPN/EPII-Plus module or the internal Safenet chip, or the IOS software is used for cryptographic operations.

The cryptographic boundary of the module is the device's case. All of the functionality discussed in this document is provided by components within this cryptographic boundary.

The interface for the router is located on the front and rear panels as shown in Figure 2 and Figure 3, respectively.

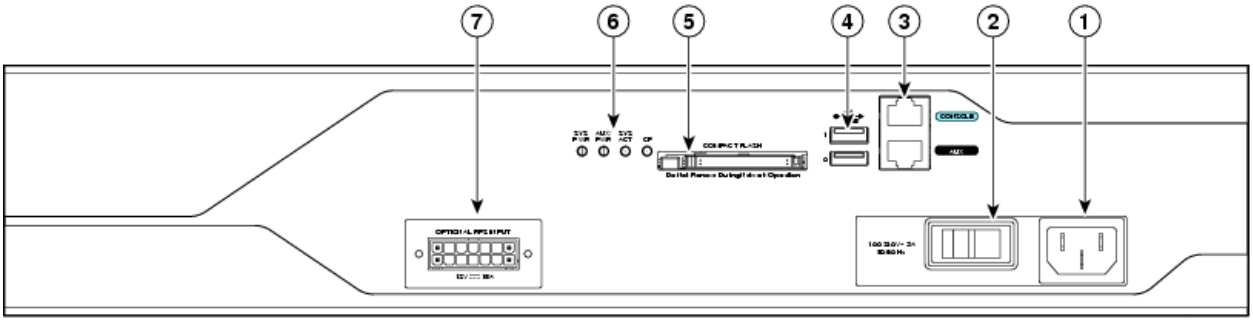

Figure 2 – Front Panel Physical Interfaces

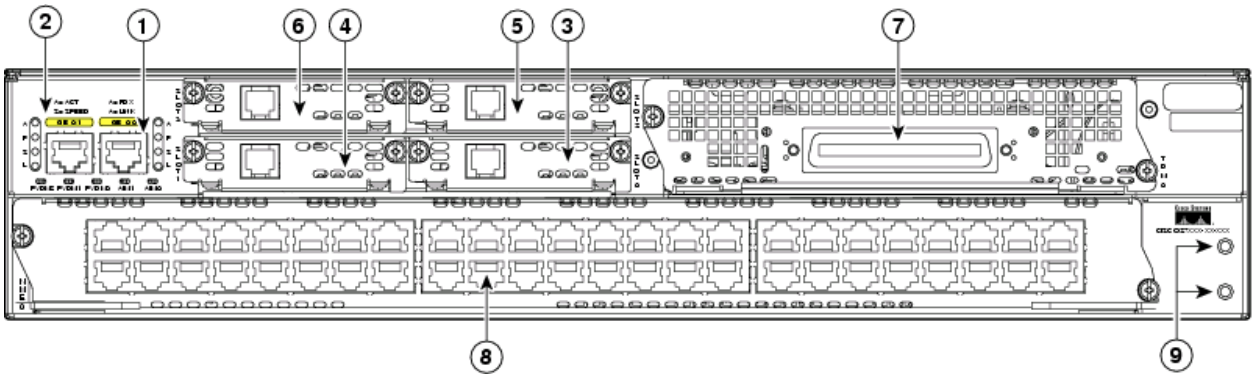

Figure 3 – Rear Panel Physical Interfaces

The Cisco 2851 router features a console port, an auxiliary port, two Universal Serial Bus (USB) ports, four high-speed WAN interface card (HWIC) slots, two10/100 Gigabit Ethernet RJ45 ports, a Enhanced Network Module (ENM) slot, a Voice Network Module (VeNoM) slot, and a Compact Flash (CF) drive. The 2851 router supports one single-width network module, four single-width or two double-width HWICs, two slots for AIM-VPN/BPII-Plus cards[1], three internal packet voice data modules (PVDMs), two fast Ethernet connections, and 16 ports of IP phone power output. Figure 2 shows the front panel and Figure 3 shows the rear panel. The front panel contains 4 LEDs that output status data about the system power, auxiliary power, system activity, and compact flash busy status. The back panel consists of 13 LEDs: two Ethernet activity LEDs, two duplex LEDs, two speed LEDs, two link LEDs, three PVDM LEDs, and two AIM LEDs.

The front panel contains the following:

- (1) Power inlet
- (2) Power switch
- (3) Console and auxiliary ports
- (4) USB ports
- (5) CF drive
- (6) LEDs described in table 1.
- (7) Optional RPS input

The back panel contains the following:

- (1) GE 0 port
- (2) GE 1 port
- (3) HWIC 0 slot
- (4) HWIC 1 slot
- (5) HWIC 2 slot
- (6) HWIC 3 slot
- (7) VeNoM slot
- (8) ENM slot
- (9) Ground connector

[1] The security policy covers the configuration in which one AIM card is used.

The following tables provide more detailed information conveyed by the LEDs on the front and rear panel of the router:

Name	State	Description
System Power	Off Blinking Green Solid Green Solid Orange	Power off ROMMON mode Operating normally System Error Detected
Auxiliary Power	Off Solid Green Solid Orange	-48V PS and RPS not present -48V PS or RPS present and functional -48V PS or RPS present and failure detected
Activity	Off Blinking Green Solid Green	No interrupts or packet transfer occurring System is servicing interrupts System is actively transferring packets
Compact Flash	Off Solid Green	No ongoing accesses, eject permitted Device is busy, do not eject

Table 1 – 2851 Front Panel Indicators

Name	State	Description
PVDM2	Off Solid Green Solid Orange	PVDM2 not installed PVDM2 installed and initialized PVDM2 installed and initialized error
PVDM1	Off Solid Green Solid Orange	PVDM1 not installed PVDM1 installed and initialized PVDM1 installed and initialized error
PVDM0	Off Solid Green Solid Orange	PVDM0 not installed PVDM0 installed and initialized PVDM0 installed and initialized error
AIM1	Off Solid Green Solid Orange	AIM1 not installed AIM1 installed and initialized AIM1 installed and initialized error
AIM0	Off Solid Green Solid Orange	AIM0 not installed AIM0 installed and initialized AIM0 installed and initialized error

Table 2 – 2851 Rear Panel Indicators

The following table describes the meaning of Ethernet LEDs on the rear panel:

Name	State	Description
Activity	Off Solid/Blinking Green	Not receiving packets Receiving packets
Duplex	Off Solid Green	Half-Duplex Full-Duplex
Speed	One Blink Green Two Blink Green	10 Mbps 100 Mbps
Link	Off Solid Green	No link established Ethernet link is established

Table 3 – 2851 Ethernet Indicators

The physical interfaces are separated into the logical interfaces from FIPS 140-2 as described in the following table:

Router Physical Interface	FIPS 140-2 Logical Interface
10/100 Ethernet LAN Ports HWIC Ports Console Port Auxiliary Port ENM Slot VeNoM Slot USB Port	Data Input Interface
10/100 Ethernet LAN Ports HWIC Ports Console Port Auxiliary Port ENM Slot VeNoM Slot USB Port	Data Output Interface
10/100 Ethernet LAN Ports HWIC Ports Power Switch Console Port Auxiliary Port ENM Slot	Control Input Interface
10/100 Ethernet LAN Port LEDs AIM LEDs PVDM LEDs Power LED Activity LEDs Auxiliary LED Compact Flash LED Console Port Auxiliary Port USB Port	Status Output Interface
Main Power Plug Redundant Power Supply Plug	Power Interface

Table 4 – 2851 FIPS 140-2 Logical Interfaces

The CF card that stored the IOS image is considered an internal memory module, because the IOS image stored in the card may not be modified or upgraded. The card itself must never be removed from the drive. Tamper evident seal will be placed over the card in the drive.

2.2 Roles and Services

Authentication in Cisco 2851 is role-based. There are two main roles in the router that operators can assume: the Crypto Officer role and the User role. The administrator of the router assumes the Crypto Officer role in order to configure and maintain the router using Crypto Officer services, while the Users exercise only the basic User services. The module supports RADIUS and TACACS+ for authentication. A complete description of all the management and

configuration capabilities of the router can be found in the *Performing Basic System Management* manual and in the online help for the router.

2.2.1. User Services

Users enter the system by accessing the console port with a terminal program or via IPSec protected telnet or SSH session to a LAN port. The IOS prompts the User for username and password. If the password is correct, the User is allowed entry to the IOS executive program. The services available to the User role consist of the following:

Status Functions	View state of interfaces and protocols, version of IOS currently running.
Network Functions	Connect to other network devices through outgoing telnet, PPP, etc. and initiate diagnostic network services (i.e., ping, mtrace).
Terminal Functions	Adjust the terminal session (e.g., lock the terminal, adjust flow control).
Directory Services	Display directory of files kept in flash memory.
SSL-TLS/VPN	Negotiation and encrypted data transport via SSL/TLS.
EASY VPN	Negotiation and encrypted data transport via EASY VPN.

2.2.2 Crypto Officer Services

During initial configuration of the router, the Crypto Officer password (the “enable” password) is defined. A Crypto Officer can assign permission to access the Crypto Officer role to additional accounts, thereby creating additional Crypto Officers.

The Crypto Officer role is responsible for the configuration and maintenance of the router.

The Crypto Officer services consist of the following:

Configure the router	Define network interfaces and settings, create command aliases, set the protocols the router will support, enable interfaces and network services, set system date and time, and load authentication information.
Define Rules and Filters	Create packet Filters that are applied to User data streams on each interface. Each Filter consists of a set of Rules, which define a set of packets to permit or deny based on characteristics such as protocol ID, addresses, ports, TCP connection establishment, or packet direction.
View Status Functions	View the router configuration, routing tables, active sessions, use gets to view SNMP MIB statistics, health, temperature, memory status, voltage, packet statistics, review accounting logs, and view physical interface status.
Manage the router	Log off users, shutdown or reload the router, erase the flash memory, manually back up router configurations, view complete

	configurations, manager user rights, and restore router configurations.
Set Encryption/Bypass	Set up the configuration tables for IP tunneling. Set preshared keys and algorithms to be used for each IP range or allow plaintext packets to be set from specified IP address.

Bypass Mode

The routers implement an alternating bypass capability, in which some connections may be cryptographically authenticated and encrypted while others may not. Two independent internal actions are required in order to transition into each bypass state: First, the bypass state must be configured by the Crypto Officer using “match address <ACL-name>" sub-command under crypto map which defines what traffic is encrypted. Second, the module must receive a packet that is destined for an IP that is not configured to receive encrypted data. The configuration table uses an error detection code to detect integrity failures, and if an integrity error is detected, the module will enter an error state in which no packets are routed. Therefore, a single error in the configuration table cannot cause plaintext to be transmitted to an IP address for which it should be encrypted.

2.2.3 Unauthenticated Services

The services available to unauthenticated users are:

- Viewing the status output from the module’s LEDs
- Powering the module on and off using the power switch
- Sending packets in bypass

2.2.4 Strength of Authentication

The security policy stipulates that all user passwords must be 8 alphanumeric characters, so the password space is 2.8 trillion possible passwords. The possibility of randomly guessing a password is thus far less than one in one million. To exceed a one in 100,000 probability of a successful random password guess in one minute, an attacker would have to be capable of 28 million password attempts per minute, which far exceeds the operational capabilities of the module to support.

When using RSA based authentication, RSA key pair has modulus size of 1024 bit to 2048 bit, thus providing between 80 bits and 112 bits of strength. Assuming the low end of that range, an attacker would have a 1 in 280 chance of randomly obtaining the key, which is much stronger than the one in a million chance required by FIPS 140-2. To exceed a one in 100,000 probability of a successful random key guess in one minute, an attacker would have to be capable of approximately 1.8x1021 attempts per minute, which far exceeds the operational capabilities of the modules to support.

When using preshared key based authentication, the security policy stipulates that all preshared keys must be 8 alphanumeric characters, so the key space is 2.8 trillion possible combinations. The possibility of randomly guessing this is thus far less than one in one million. To exceed a

one in 100,000 probability of a successful random guess in one minute, an attacker would have to be capable of 28 million attempts per minute, which far exceeds the operational capabilities of the module to support.

2.3 Physical Security

The router is entirely encased by a metal, opaque case. The rear of the unit contains HWIC/WIC/VIC connectors, LAN connectors, a CF drive, power connector, console connector, auxiliary connector, USB port, and fast Ethernet connectors. The front of the unit contains the system status and activity LEDs. The top, side, and front portion of the chassis can be removed to allow access to the motherboard, memory, AIM slot, and expansion slots.

The Cisco 2851 routers require that a special opacity shield be installed over the side air vents in order to operate in FIPS-approved mode. The shield decreases the surface area of the vent holes, reducing visibility within the cryptographic boundary to FIPS-approved specifications.

Install the opacity plates as specified in the pictures below:

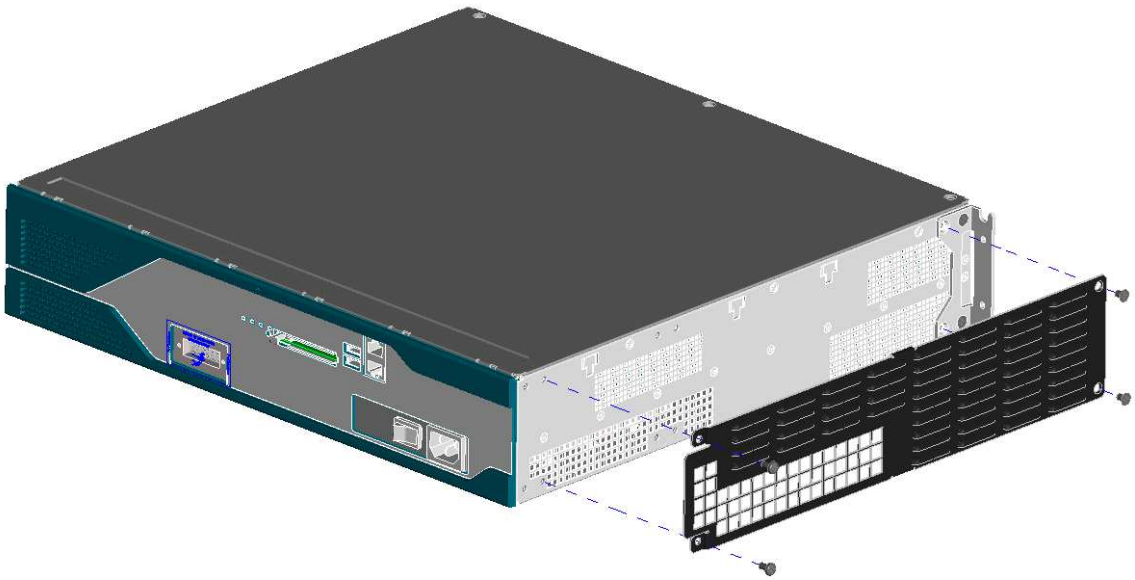

Figure 4 – 2851 – Opacity Shield Position

Once the router has been configured in to meet FIPS 140-2 Level 2 requirements, the router cannot be accessed without signs of tampering. To seal the system, apply serialized tamper-evidence labels as follows:

1. Clean the cover of any grease, dirt, or oil before applying the tamper evidence labels. Alcohol-based cleaning pads are recommended for this purpose. The temperature of the router should be above 10°C.
2. The tamper evidence label should be placed so that the one half of labels A, B, C, D and E covers the enclosure and the other half covers the port adapter slot.
3. The tamper evidence label should be placed so that the one half of label F covers the enclosure and the other half covers the rear panel.
4. The tamper evidence label should be placed so that one half of labels G and H covers the front panel and the other half covers the enclosure.
5. The tamper evidence label I should be placed over the CF card in the slot so that any attempt to remove the card will show sign of tampering.
6. Place tamper evident labels on the opacity shield as shown in Figure 7.
7. The labels completely cure within five minutes.

Figures 5, 6 and 7 show the additional tamper evidence label placements for the 2851.

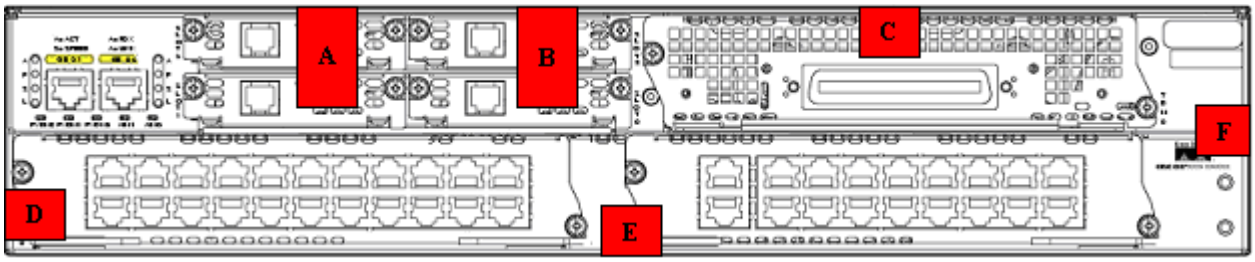

Figure 5 – 2851 Tamper Evident Label Placement (Back View)

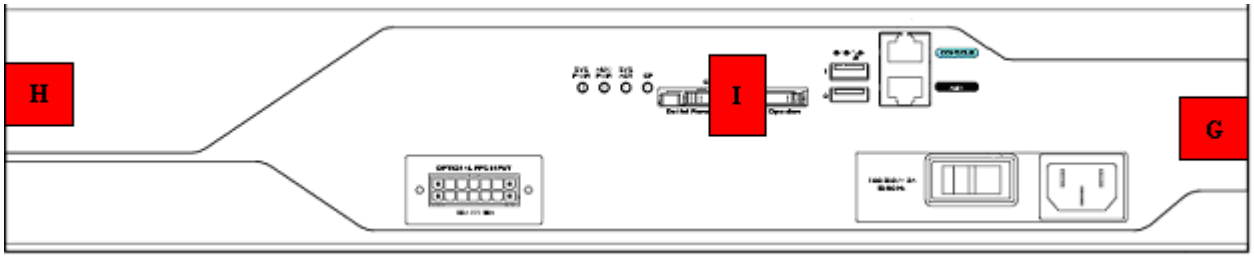

Figure 6 – 2851 Tamper Evident Label Placement (Front View)

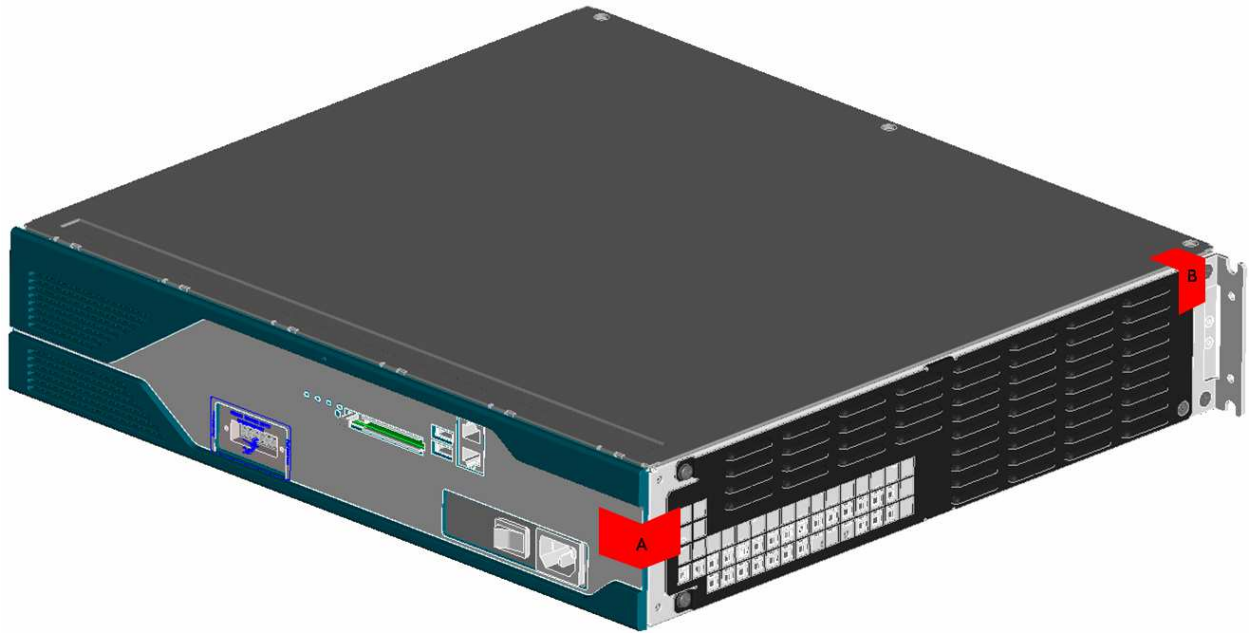

Figure 7 – 2851 Tamper Evident Label Placement on the Opacity Shield

The tamper evidence seals are produced from a special thin gauge vinyl with self-adhesive backing. Any attempt to open the router will damage the tamper evidence seals or the material of the module cover. Since the tamper evidence seals have non-repeated serial numbers, they can be inspected for damage and compared against the applied serial numbers to verify that the module has not been tampered. Tamper evidence seals can also be inspected for signs of tampering, which include the following: curled corners, bubbling, crinkling, rips, tears, and slices. The word "OPEN" may appear if the label was peeled back.

2.4 Cryptographic Key Management

The router securely administers both cryptographic keys and other critical security parameters such as passwords. The tamper evidence seals provide physical protection for all keys. All keys are also protected by the password-protection on the Crypto Officer role login, and can be zeroized by the Crypto Officer. All zeroization consists of overwriting the memory that stored the key. Keys are exchanged and entered electronically or via Internet Key Exchange (IKE) or SSL handshake protocols.

The routers support the following FIPS-2 approved algorithm implementations:

Algorithm	Algorithm Certificate Number
Software (IOS) Implementations	
AES	795
Triple-DES	683
SHA-1, SHA-256, SHA-512	794
HMAC-SHA-1	436
X9.31 PRNG	456

RSA	379
Onboard Safenet Implementations	
AES	96
Triple-DES	210
SHA-1	317
HMAC-SHA-1	50
AIM Module Implementations	
AES	100
Triple-DES	213
SHA-1	401
HMAC-SHA-1	38
X9.31 PRNG	80
RSA	383

The router is in the approved mode of operation only when FIPS 140-2 approved algorithms are used (except DH and RSA key transport which are allowed in the approved mode for key establishment despite being non-approved).

Note: The module supports DH key sizes of 1024 and 1536 bits and RSA key sizes of 1024, 1536 and 2048 bits. Therefore, the Diffie Hellmann Key agreement, key establishment methodology provides between 80-bits and 96-bits of encryption strength per NIST 800-57. RSA Key wrapping, key establishment methodology provides between 80-bits and 112-bits of encryption strength per NIST 800-57.

The following are not FIPS 140-2 approved Algorithms: DES, RC4, MD5, HMAC-MD5, RSA key wrapping and DH; however again DH and RSA are allowed for use in key establishment.

The module contains a HiFn 7814-W cryptographic accelerator chip, integrated in the AIM card. Unless the AIM card is disabled by the Crypto Officer with the “no crypto engine aim” command, the HiFn 7814-W provides AES (128-bit, 192-bit, and 256-bit) and Triple-DES (168-bit) encryption; MD5 and SHA-1 hashing; and hardware support for DH, X9.31 RNG, RSA encryption/decryption, and RSA public key signature/verification.

The module supports the following types of key management schemes:

1. Pre-shared key exchange via electronic key entry. Triple-DES/AES key and HMAC-SHA-1 key are exchanged and entered electronically.
2. Internet Key Exchange method with support for pre-shared keys exchanged and entered electronically.
    - The pre-shared keys are used with Diffie-Hellman key agreement technique to derive Triple-DES or AES keys.
    - The pre-shared key is also used to derive HMAC-SHA-1 key.
3. RSA digital signatures based authentication is used for IKE, with Diffie-Hellman Key agreement technique to derive AES or Triple-DES keys.
4. RSA encrypted nonces based authentication is used for IKE, with Diffie-Hellman Key agreement technique to derive AES or Triple-DES keys.

5. RSA key transport is used to derive the Triple-DES or AES keys during SSLv3.1/TLS handshake.

The module supports commercially available Diffie-Hellman and RSA key transport for key establishment.

All pre-shared keys are associated with the CO role that created the keys, and the CO role is protected by a password. Therefore, the CO password is associated with all the pre-shared keys. The Crypto Officer needs to be authenticated to store keys. All Diffie-Hellman (DH) keys agreed upon for individual tunnels are directly associated with that specific tunnel only via the IKE protocol. RSA Public keys are entered into the modules using digital certificates which contain relevant data such as the name of the public key's owner, which associates the key with the correct entity. All other keys are associated with the user/role that entered them.

Key Zeroization:
Each key can be zeroized by sending the "no" command prior to the key function commands. This will zeroize each key from the DRAM, the running configuration.

"Clear Crypto IPSec SA" will zeroize the Triple-DES/AES session key (which is derived using the Diffie-Hellman key agreement technique) from the DRAM. This session key is only available in the DRAM; therefore this command will completely zeroize this key. The following command will zeroize the pre-shared keys from the DRAM:

- no set session-key inbound ah spi hex-key-data
- no set session-key outbound ah spi hex-key-data
- no set session-key inbound esp spi cipher hex-key-data [authenticator hex-key-data]
- no set session-key outbound esp spi cipher hex-key-data [authenticator hex-key-data]
- no crypto isakmp key

The DRAM running configuration must be copied to the start-up configuration in NVRAM in order to completely zeroize the keys.

The RSA keys are zeroized by issuing the CLI command "crypto key zeroize rsa".
All SSL/TLS session keys are zeroized automatically at the end of the SSL/TLS session.

The module supports the following keys and critical security parameters (CSPs).

Key/CSP Name	Algorithm	Description	Storage Location	Zeroization Method
PRNG Seed	X9.31	This is the seed for X9.31 PRNG. This CSP is stored in DRAM and updated periodically after the generation of 400 bytes – after this it is reseeded with router-derived entropy; hence, it is zeroized periodically. Also, the operator can turn off the router to zeroize this	DRAM	Automatically every 400 bytes, or turn off the router.

		CSP.		
PRNG Seed key	X9.31	This is the seed key for the X9.31 PRNG	DRAM	Turn off the router
Diffie Hellman private exponent	DH	The private exponent used in Diffie-Hellman (DH) exchange as part of IKE. Zeroized after DH shared secret has been generated.	DRAM	Automatically after shared secret generated.
Diffie Hellman public key	DH	The public key used in Diffie-Hellman (DH) exchange as part of IKE. Zeroized after the DH shared secret has been generated.	DRAM	Automatically after shared secret generated.
skeyid	Keyed SHA-1	Value derived from the shared secret within IKE exchange. Zeroized when IKE session is terminated.	DRAM	Automatically after IKE session terminated.
skeyid_d	Keyed SHA-1	The IKE key derivation key for non ISAKMP security associations.	DRAM	Automatically after IKE session terminated.
skeyid_a	HMAC-SHA-1	The ISAKMP security association authentication key.	DRAM	Automatically after IKE session terminated.
skeyid_e	TRIPLE-DES/AES	The ISAKMP security association encryption key.	DRAM	Automatically after IKE session terminated.
IKE session encrypt key	TRIPLE-DES/AES	The IKE session encrypt key.	DRAM	Automatically after IKE session terminated.
IKE session authentication key	HMAC-SHA-1	The IKE session authentication key.	DRAM	Automatically after IKE session terminated.
ISAKMP preshared	Shared secret	The key used to generate IKE skeyid during preshared-key authentication. “no crypto isakmp key” command zeroizes it. This key can have two forms based on whether the key is related to the hostname or the IP address.	NVRAM	“# no crypto isakmp key”
IKE hash key	HMAC-SHA-1	This key generates the IKE shared secret keys. This key is zeroized after generating those keys.	DRAM	Automatically after generating IKE shared secret keys.
IKE RSA Authentication private Key	RSA	RSA private key for IKE authentication. Generated or entered like any RSA key, set as IKE RSA Authentication Key with the “crypto keyring” or “ca trust-point” command.	NVRAM	“# crypto key zeroize rsa"

IKE RSA Authentication Public Key	RSA	RSA public key for IKE authentication. Generated or entered like any RSA key, set as IKE RSA Authentication Key with the “crypto keyring” or “ca trust-point” command.	NVRAM	“# crypto key zeroize rsa"
IKE RSA Encrypted Nonce Private Key	RSA	RSA private key for IKE encrypted nonces. Generated like any RSA, with the “usage-keys” parameter included.	NVRAM	“# crypto key zeroize rsa"
IKE RSA Encrypted Nonce Public Key	RSA	RSA public key for IKE encrypted nonces. Generated like any RSA, with the “usage-keys” parameter included.	NVRAM	“# crypto key zeroize rsa"
IPSec encryption key	DES/TRIPLE-DES/AES	The IPSec encryption key. Zeroized when IPSec session is terminated.	DRAM	“# Clear Crypto IPSec SA”
IPSec authentication key	HMAC-SHA-1	The IPSec authentication key. The zeroization is the same as above.	DRAM	“# Clear Crypto IPSec SA”
Configuration encryption key	AES	The key used to encrypt values of the configuration file. This key is zeroized when the “no key config-key” is issued. Note that this command does **not** decrypt the configuration file, so zeroize with care.	NVRAM	“# no key config-key”
Router authentication key 1	Shared secret	This key is used by the router to authenticate itself to the peer. The router itself gets the password (that is used as this key) from the AAA server and sends it onto the peer. The password retrieved from the AAA server is zeroized upon completion of the authentication attempt.	DRAM	Automatically upon completion of authentication attempt.
PPP authentication key	RFC 1334	The authentication key used in PPP. This key is in the DRAM and not zeroized at runtime. One can turn off the router to zeroize this key because it is stored in DRAM.	DRAM	Turn off the router.
Router authentication key 2	Shared Secret	This key is used by the router to authenticate itself to the peer. The key is identical to Router authentication key 1 except that it is retrieved from the local database (on the router itself). Issuing the “no username password” zeroizes the password (that is used as this key) from the local database.	NVRAM	“# no username password”
SSH session key	Various symmetric	This is the SSH session key. It is zeroized when the SSH session is terminated.	DRAM	Automatically when SSH session terminated

User password	Shared Secret	The password of the User role. This password is zeroized by overwriting it with a new password.	NVRAM	Overwrite with new password
Enable password	Shared Secret	The plaintext password of the CO role. This password is zeroized by overwriting it with a new password.	NVRAM	Overwrite with new password
Enable secret	Shared Secret	The ciphertext password of the CO role. However, the algorithm used to encrypt this password is not FIPS approved. Therefore, this password is considered plaintext for FIPS purposes. This password is zeroized by overwriting it with a new password.	NVRAM	Overwrite with new password
RADIUS secret	Shared Secret	The RADIUS shared secret. This shared secret is zeroized by executing the “no radius-server key” command.	NVRAM	“# no radius-server key”
secret_1_0_0		The fixed key used in Cisco vendor ID generation. This key is embedded in the module binary image and can be deleted by erasing the Flash.	NVRAM	Deleted by erasing the Flash.
TACACS+ secret	Shared Secret	The TACACS+ shared secret. This shared secret is zeroized by executing the “no tacacs-server key” command.	NVRAM	“# no tacacs-server key”
TLS server private key	RSA	1024/1536/2048 bit RSA private key used for SSLV3.1/TLS.	NVRAM	“# crypto key zeroize rsa"
TLS server public key	RSA	1024/1536/2048 bit RSA public key used for SSLV3.1/TLS.	NVRAM	“# crypto key zeroize rsa"
TLS pre-master secret	Shared Secret	Shared Secret created using asymmetric cryptography from which new TLS session keys can be created	DRAM	Automatically when TLS session is terminated
TLS Encryption Key	AES/TRIPLE-DES	Key used to encrypt TLS session data	DRAM	Automatically when TLS session is terminated
TLS Integrity Key	HMAC-SHA-1	HMAC-SHA-1 used for TLS data integrity protection	DRAM	Automatically when TLS session is terminated

Table 5 - Cryptographic Keys and CSPs

SRDI/Role/Service Access Policy (r = read, w = write, d = delete)	Roles/Service	**User Role**	Status Functions	Network Functions	Terminal Functions	Directory Services	SSL-TLS/VPN	EASY VPN	**Crypto Officer Role**	Configure the Router	Define Rules and Filters	Status Functions	Manage the Router	Set Encryption/Bypass	Change WAN Interface Cards
Security Relevant Data Item															
PRNG Seed				r									d	r w d	
PRNG Seed Key				r									d	r w d	
Diffie Hellman private exponent				r										r w d	
Diffie Hellman public key				r										r w d	
skeyid				r				r w d						r w d	
skeyid_d				r				r w d						r w d	
skeyid_a				r				r w d						r w d	
skeyid_e				r				r w d						r w d	
IKE session encrypt key				r				r w d						r w d	
IKE session authentication key				r				r w d						r w d	
ISAKMP preshared				r				r w d						r w d	
IKE hash key				r				r w d						r w d	
IKE RSA Authentication private Key				r				r w d		r w				r w d	

IKE RSA Authentication Public Key				r				r w d		r w				r w d	
IKE RSA Encrypted Nonce Private Key				r				r w d		r w				r w d	
IKE RSA Encrypted Nonce Public Key				r				r w d		r w				r w d	
IPSec encryption key				r				r w d						r w d	
IPSec authentication key				r				r w d						r w d	
Configuration encryption key										r w d			r w d		
Router authentication key 1				r									r w d		
PPP authentication key				r									d	r w	
Router authentication key 2				r						r w d					
SSH session key				r										r w d	
User password				r									r w d		
Enable password													r w d		
Enable secret													r w d		
RADIUS secret													r w d		
secret_1_0_0										r w d					
TACACS+ secret														r w d	
TLS server private key				r			r w d			r w				r w d	
TLS server public key				r			r w d			r w				r w d	

TLS pre-master secret				r			r w d							r w d	
TLS Encryption Key				r			r w d							r w d	
TLS Integrity Key				r			r w d							r w d	

Table 6 – Role and Service Access to CSP

2.5 Self-Tests

In order to prevent any secure data from being released, it is important to test the cryptographic components of a security module to insure all components are functioning correctly. The router includes an array of self-tests that are run during startup and periodically during operations. All self-tests are implemented by the software. An example of self-tests run at power-up is a cryptographic known answer test (KAT) on each of the FIPS-approved cryptographic algorithms and on the Diffie-Hellman algorithm. Examples of tests performed at startup are a software integrity test using an EDC. Examples of tests run periodically or conditionally include: a bypass mode test performed conditionally prior to executing IPSec, and a continuous random number generator test. If any of the self-tests fail, the router transitions into an error state. In the error state, all secure data transmission is halted and the router outputs status information indicating the failure.

Examples of the errors that cause the system to transition to an error state:

- IOS image integrity checksum failed
- Microprocessor overheats and burns out
- Known answer test failed
- NVRAM module malfunction.
- Temperature high warning

2.5.1 Self-tests performed by the IOS image

- IOS Self Tests
    - POST tests
        - AES Known Answer Test
        - RSA Signature Known Answer Test (both signature/verification)
        - Software/firmware test
        - Power up bypass test
        - RNG Known Answer Test
        - Diffie Hellman test
        - HMAC-SHA-1 Known Answer Test
        - SHA-1/256/512 Known Answer Test
        - Triple-DES Known Answer Test
    - Conditional tests
        - Pairwise consistency test for RSA signature keys
        - Conditional bypass test
        - Continuous random number generation test for approved and non-approved RNGs.

2.5.2 Self-tests performed by AIM

- AIM Self Tests[2]
  - POST tests
    - AES Known Answer Test
    - Triple-DES Known Answer Test
    - SHA-1 Known Answer Test
    - HMAC-SHA-1 Known Answer Test
    - RNG Known Answer Test
    - Firmware integrity test
    - Diffie Hellman Test
    - RSA signature gen/ver known answer test
  - Conditional Tests
    - Pairwise consistency test for RSA signature keys
    - Continuous RNG test for the hardware RNG

2.5.3 Self-tests performed by Safenet[3]

- Safenet Self Tests
  - POST tests
    - AES Known Answer Test
    - Triple-DES Known Answer Test
    - HMAC-SHA-1 Known Answer Test
    - SHA-1 Known Answer Test

3 Secure Operation of the Cisco 2851 router

The Cisco 2851 routers meet all the Level 2 requirements for FIPS 140-2. Follow the setting instructions provided below to place the module in FIPS-approved mode. Operating this router without maintaining the following settings will remove the module from the FIPS approved mode of operation.

3.1 Initial Setup

1. The Crypto Officer must apply tamper evidence labels as described in Section 2.4 of this document.
2. The Crypto Officer must disable IOS Password Recovery by executing the following commands:

```
configure terminal
no service password-recovery
end
show version
```

[2] Unless disabled by Crypto Officer.
[3] Unless disabled by Crypto Officer.

NOTE: Once Password Recovery is disabled, administrative access to the module without the password will not be possible.

3.2 System Initialization and Configuration

1. The Crypto Officer must perform the initial configuration. IOS version 12.4 (15) T3, Advanced Security build (advsecurity) is the only allowable image; no other image should be loaded.
2. The value of the boot field must be 0x0102. This setting disables break from the console to the ROM monitor and automatically boots the IOS image. From the "configure terminal" command line, the Crypto Officer enters the following syntax:

```
config-register 0x0102
```

3. The Crypto Officer must create the "enable" password for the Crypto Officer role. The password must be at least 8 characters (all digits; all lower and upper case letters; and all special characters except '?' are accepted) and is entered when the Crypto Officer first engages the "enable" command. The Crypto Officer enters the following syntax at the "#" prompt:

```
enable secret [PASSWORD]
```

4. The Crypto Officer must always assign passwords (of at least 8 characters) to users. Identification and authentication on the console port is required for Users. From the "configure terminal" command line, the Crypto Officer enters the following syntax:

```
line con 0
password [PASSWORD]
login local
```

5. RADIUS and TACACS+ shared secret key sizes must be at least 8 characters long.

3.3 IPSec Requirements and Cryptographic Algorithms

1. The only type of key management that is allowed in FIPS mode is Internet Key Exchange (IKE).
2. Although the IOS implementation of IKE allows a number of algorithms, only the following algorithms are allowed in a FIPS 140-2 configuration:

   ah-sha-hmac

   esp-sha-hmac

   esp-Triple-DES

   esp-aes

3. The following algorithms are not FIPS approved and should not be used during FIPS-approved mode:

   DES

   MD-5 for signing

MD-5 HMAC

3.4 Protocols

1. SNMP v3 over a secure IPSec tunnel may be employed for authenticated, secure SNMP *gets* and *sets*. Since SNMP v2C uses community strings for authentication, only *gets* are allowed under SNMP v2C.

3.5 SSLv3.1/TLS Requirements and Cryptographic Algorithms

When negotiating SSLv3.1/TLS cipher suites, only FIPS approved algorithms must be specified.

All other versions of SSL except version 3.1 must not be used in FIPS mode of operation

The following algorithms are not FIPS approved and should not be used in the FIPS-approved mode:

MD5

RC4

RC2

DES

3.6 Remote Access

1. Telnet access to the module is only allowed via a secure IPSec tunnel between the remote system and the module. The Crypto officer must configure the module so that any remote connections via telnet are secured through IPSec, using FIPS-approved algorithms. Note that all users must still authenticate after remote access is granted.
2. SSH access to the module is only allowed if SSH is configured to use a FIPS-approved algorithm. The Crypto officer must configure the module so that SSH uses only FIPS-approved algorithms. Note that all users must still authenticate after remote access is granted.

CISCO EDITOR'S NOTE: You may now include all standard Cisco information included in all documentation produced by Cisco. Be sure that the following line is in the legal statements at the end of the document:

> *By printing or making a copy of this document, the user agrees to use this information for product evaluation purposes only. Sale of this information in whole or in part is not authorized by Cisco Systems.*